

C L A I M S

1. An encrypted communication method
2 characterized by comprising the steps of:
3 a) causing a communication method resolution
4 unit to determine on the basis of a domain name
5 contained in one of a name resolution query transmitted
6 from an application that communicates with a node
7 apparatus connected to a network to resolve an IP
8 address of the node apparatus and a name resolution
9 response as a response to the name resolution query
10 whether the node apparatus is an encrypted communication
11 target node;
12 b) causing an encrypted communication path
13 setting unit to register the IP address of the node
14 apparatus in an encrypted communication path setting
15 table when the node apparatus is the encrypted
16 communication target node;
17 c) causing a name resolution query/response
18 transmission/reception unit to transmit the IP address
19 of the node apparatus contained in the name resolution
20 response to the application;
21 d) causing the application to transmit a data
22 packet in which the IP address of the node apparatus is
23 set as a destination address; and
24 e) causing a data transmission/reception unit
25 to receive the data packet transmitted from the
26 application and, if a communication partner IP address

27 set as the destination address of the data packet is
28 registered in the encrypted communication path setting
29 table, encrypt and transmit the data packet.

2 2. An encrypted communication method
3 according to claim 1, characterized in that processes of
4 the step a, the step b, and the step c are executed by a
5 name resolution proxy unit provided in a node apparatus
in which the application operates.

2 3. An encrypted communication method
3 according to claim 1, characterized in that a process of
4 the step a is executed by a name resolution server, and
5 processes of the step b and the step c are executed by a
6 name resolution proxy unit provided in a node apparatus
in which the application operates.

2 4. An encrypted communication method
3 according to claim 1, characterized in that the
4 communication method resolution unit determines whether
5 the node apparatus is an encrypted communication target
6 node by looking up a setting table in which at least
part of the domain name of the encrypted communication
7 target node is registered.

2 5. An encrypted communication method
3 characterized by comprising the steps of:
4 a) causing a communication method resolution
5 unit to determine on the basis of a domain name
6 contained in one of a name resolution query transmitted
from an application on a client node to resolve an IP

7 address of another node apparatus serving as a
8 communication target of the application and a name
9 resolution response as a response to the name resolution
10 query whether said other node apparatus is an encrypted
11 communication target node;

12 b) causing an encrypted communication path
13 setting unit to register, in an encrypted communication
14 path setting table, a correspondence between the IP
15 address of said other node apparatus and an intercept
16 address that is not used in any other communication
17 session when said other node apparatus is the encrypted
18 communication target node;

19 c) causing a name resolution query/response
20 transmission/reception unit to transmit, to the
21 application as the name resolution response, an
22 intercept address corresponding to the IP address of
23 said other node apparatus contained in the name
24 resolution response;

25 d) causing the application to transmit a data
26 packet in which the intercept address is set as a
27 destination address; and

28 e) causing a data transmission/reception unit
29 to receive the data packet transmitted from the
30 application, read out, from the encrypted communication
31 path setting table, a communication partner IP address
32 corresponding to the intercept address set as the
33 destination address of the data packet, set the readout

34 communication partner IP address as the destination
35 address of the data packet, and encrypt and transmit the
36 set data packet.

6. An encrypted communication method
2 according to claim 5, characterized in that processes of
3 the step a, the step b, and the step c are executed by a
4 name resolution proxy unit provided in a communication
5 encryption node apparatus having the data
6 transmission/reception unit.

7. An encrypted communication method
2 according to claim 5, characterized in that a process of
3 the step a is executed by a name resolution server, and
4 processes of the step b and the step c are executed by a
5 name resolution proxy unit provided in a communication
6 encryption node apparatus having the data
7 transmission/reception unit.

8. An encrypted communication method
2 according to claim 5, characterized in that the
3 communication method resolution unit determines whether
4 said other node apparatus is an encrypted communication
5 target node by looking up a setting table in which at
6 least part of the domain name of the encrypted
7 communication target node is registered.

9. A node apparatus characterized by
2 comprising:
3 an application that communicates with another
4 node apparatus connected to a network;

5 a data transmission/reception unit provided in
6 a kernel unit; and
7 a name resolution proxy unit which relays a
8 name resolution query transmitted from said application
9 to a name resolution server to resolve an IP address of
10 said other node apparatus and a name resolution response
11 as a response to the name resolution query,
12 said data transmission/reception unit
13 comprising
14 an encrypted communication path setting table
15 which holds a communication partner IP address, and
16 a communication encryption unit which receives
17 a data packet transmitted from said application and
18 encrypts and transmits the data packet when a
19 communication partner IP address set as the destination
20 address of the data packet is registered in said
21 encrypted communication path setting table, and
22 said name resolution proxy unit comprising an
23 encrypted communication path setting unit which
24 registers, in said encrypted communication path setting
25 table, the IP address of said other node apparatus
26 resolved by the name resolution response if it is
27 determined on the basis of a domain name of said other
28 node apparatus contained in one of the name resolution
29 query and the name resolution response that said other
30 node apparatus is an encrypted communication target
31 node.

10. A node apparatus according to claim 9,
2 characterized in that said encrypted communication path
3 setting table holds a plurality of communication partner
4 IP addresses.

11. A node apparatus according to claim 9,
2 characterized in that said name resolution proxy unit
3 further comprises a communication method resolution unit
4 which determines on the basis of the domain name of said
5 other node apparatus whether said other node apparatus
6 is the encrypted communication target node.

12. A node apparatus according to claim 11,
2 characterized in that

3 said encrypted communication path setting
4 table holds encrypted communication path setting
5 information to be used for communication with a
6 communication partner in correspondence with the
7 communication partner IP address,

8 said communication encryption unit reads out
9 corresponding encrypted communication path setting
10 information from said encrypted communication path
11 setting table, encrypts the data packet in accordance
12 with the readout encrypted communication path setting
13 information, and transmits the data packet when the
14 communication partner IP address set as the destination
15 address of the received data packet is registered in
16 said encrypted communication path setting table,
17 said name resolution proxy unit further

13. A node apparatus according to claim 9,
2 characterized in that said name resolution proxy unit
3 further comprises a name resolution query/response
4 transmission/reception unit which transmits, to the name
5 resolution server, the name resolution query transmitted
6 from said application to resolve the IP address of said
7 other node apparatus, receives, from the name resolution
8 server, the name resolution response containing a
9 determination result indicating whether said other node
10 apparatus is an encrypted communication target node and
11 the IP address of said other node apparatus, and
12 transmits, to said application, the name resolution

13 response containing the IP address of said other node
14 apparatus contained in the name resolution response.

14. A node apparatus according to claim 13,
2 characterized in that

3 said encrypted communication path setting
4 table holds encrypted communication path setting
5 information to be used for communication with a
6 communication partner in correspondence with the
7 communication partner IP address,

8 said communication encryption unit reads out
9 corresponding encrypted communication path setting
10 information from said encrypted communication path
11 setting table, encrypts the data packet in accordance
12 with the readout encrypted communication path setting
13 information, and transmits the data packet when the
14 communication partner IP address set as the destination
15 address of the received data packet is registered in
16 said encrypted communication path setting table,

17 said name resolution query/response
18 transmission/reception unit receives, from the name
19 resolution server, the name resolution response further
20 containing encrypted communication path setting
21 information in addition to the determination result and
22 the IP address of said other node apparatus, and

23 said encrypted communication path setting unit
24 registers, in said encrypted communication path setting
25 table, encrypted communication path setting information

26 contained in the name resolution response in
27 correspondence with the IP address of said other node
28 apparatus.

15. A node apparatus according to claim 11,
2 characterized in that said communication method
3 resolution unit determines whether said other node
4 apparatus is an encrypted communication target node by
5 looking up a setting table in which at least part of the
6 domain name of the encrypted communication target node
7 is registered.

16. A communication encryption node apparatus
2 connected, through a network, to a client node apparatus
3 in which an application that communicates with another
4 node apparatus connected to the network operates,
5 characterized by comprising:

6 a data transmission/reception unit provided in
7 a kernel unit; and

8 a name resolution proxy unit which relays a
9 name resolution query transmitted from the application
10 to a name resolution server to resolve an IP address of
11 said other node apparatus and a name resolution response
12 as a response to the name resolution query,

13 said data transmission/reception unit
14 comprising

15 an encrypted communication path setting table
16 which holds a correspondence between a communication
17 partner IP address and an intercept address, and

18 a communication encryption unit which receives
19 a data packet transmitted from the application, reads
20 out, from said encrypted communication path setting
21 table, a communication partner IP address corresponding
22 to an intercept address set as a destination address of
23 the data packet, sets the readout communication partner
24 IP address as the destination address of the data
25 packet, and encrypts and transmits the set data packet,
26 and

27 said name resolution proxy unit comprising
28 an encrypted communication path setting unit
29 which registers, in said encrypted communication path
30 setting table, a correspondence between the IP address
31 of said other node apparatus resolved by the name
32 resolution response and an intercept address that is not
33 used in any other communication session if it is
34 determined on the basis of a domain name of said other
35 node apparatus contained in one of the name resolution
36 query and the name resolution response that said other
37 node apparatus is an encrypted communication target
38 node, and

39 a name resolution query/response
40 transmission/reception unit which transmits, to the
41 application as the name resolution response, the
42 intercept address corresponding to the IP address of
43 said other node apparatus contained in the name
44 resolution response received from the name resolution

45 server.

17. A communication encryption node apparatus
2 according to claim 16, characterized in that said
3 encrypted communication path setting table holds a
4 plurality of correspondences between the communication
5 partner IP address and the intercept address.

18. A communication encryption node apparatus
2 according to claim 16, characterized in that said name
3 resolution proxy unit further comprises a communication
4 method resolution unit which determines on the basis of
5 the domain name of said other node apparatus whether
6 said other node apparatus is the encrypted communication
7 target node.

19. A communication encryption node apparatus
2 according to claim 17, characterized in that
3 said encrypted communication path setting
4 table holds encrypted communication path setting
5 information to be used for communication with a
6 communication partner in correspondence with the
7 communication partner IP address and the intercept
8 address,

9 said communication encryption unit reads out,
10 from said encrypted communication path setting table,
11 encrypted communication path setting information and the
12 communication partner IP address corresponding to the
13 intercept address set as the destination address of the
14 received data packet, encrypts the data packet having

15 the readout communication partner IP address set as the
16 destination address in accordance with the readout
17 encrypted communication path setting information, and
18 transmits the data packet,

19 said name resolution proxy unit further
20 comprises a setting table which holds a correspondence
21 between a domain name condition to specify an encrypted
22 communication target node and encrypted communication
23 path setting information,

24 said communication method resolution unit
25 determines that said other node apparatus is the
26 encrypted communication target node when the domain name
27 of said other node apparatus matches any one of domain
28 name conditions held in said setting table, and

29 said encrypted communication path setting unit
30 registers, in said encrypted communication path setting
31 table, encrypted communication path setting information
32 corresponding to the matched domain name condition in
33 correspondence with the IP address of said other node
34 apparatus and the intercept address.

20. A communication encryption node apparatus
2 according to claim 16, characterized in that said name
3 resolution query/response transmission/reception unit
4 transmits, to the name resolution server, the name
5 resolution query transmitted from the application to
6 resolve the IP address of said other node apparatus,
7 receives, from the name resolution server, the name

8 resolution response containing a determination result
9 indicating whether said other node apparatus is an
10 encrypted communication target node and the IP address
11 of said other node apparatus, and replaces the IP
12 address of said other node apparatus contained in the
13 name resolution response with the intercept address and
14 transmits the name resolution response to the
15 application if it is determined that said other node
16 apparatus is the encrypted communication target node.

21. A communication encryption node apparatus
2 according to claim 20, characterized in that
3 said encrypted communication path setting
4 table holds encrypted communication path setting
5 information to be used for communication with a
6 communication partner in correspondence with the
7 communication partner IP address and the intercept
8 address,

9 said communication encryption unit reads out,
10 from said encrypted communication path setting table,
11 encrypted communication path setting information and the
12 communication partner IP address corresponding to the
13 intercept address set as the destination address of the
14 received data packet, encrypts the data packet having
15 the readout communication partner IP address set as the
16 destination address in accordance with the readout
17 encrypted communication path setting information, and
18 transmits the data packet,

19 said name resolution query/response
20 transmission/reception unit receives, from the name
21 resolution server, the name resolution response further
22 containing encrypted communication path setting
23 information in addition to the determination result and
24 the IP address of said other node apparatus, and
25 said encrypted communication path setting unit
26 registers, in said encrypted communication path setting
27 table, encrypted communication path setting information
28 contained in the name resolution response in
29 correspondence with the IP address of said other node
30 apparatus and the intercept address.

22. A communication encryption node apparatus
2 according to claim 18, characterized in that said
3 communication method resolution unit determines whether
4 said other node apparatus is an encrypted communication
5 target node by looking up a setting table in which at
6 least part of the domain name of the encrypted
7 communication target node is registered.

23. An encrypted communication system
2 characterized by comprising:
3 a node apparatus in which an application that
4 communicates with another node apparatus connected to a
5 network operates; and
6 a name resolution server which resolves an IP
7 address of each of said node apparatuses,
8 said node apparatus comprising

9 a data transmission/reception unit provided in
10 a kernel unit, and
11 a name resolution proxy unit which relays a
12 name resolution query transmitted from the application
13 to said name resolution server to resolve the IP address
14 of said other node apparatus and a name resolution
15 response as a response to the name resolution query,
16 said data transmission/reception unit
17 comprising
18 an encrypted communication path setting table
19 which holds a communication partner IP address, and
20 a communication encryption unit which receives
21 a data packet transmitted from the application and
22 encrypts and transmits the data packet when a
23 communication partner IP address set as the destination
24 address of the data packet is registered in said
25 encrypted communication path setting table,
26 said name resolution server comprising a
27 communication method resolution unit which determines on
28 the basis of a domain name of said other node apparatus
29 contained in one of the name resolution query and the
30 name resolution response whether said other node
31 apparatus is an encrypted communication target node, and
32 said name resolution proxy unit comprising an
33 encrypted communication path setting unit which
34 registers, in said encrypted communication path setting
35 table, the IP address of said other node apparatus

36 resolved by the name resolution response if said other
37 node apparatus is an encrypted communication target
38 node.

24. An encrypted communication system
2 according to claim 23, characterized in that said
3 encrypted communication path setting table holds a
4 plurality of communication partner IP addresses.

25. An encrypted communication system
2 according to claim 23, characterized in that
3 said encrypted communication path setting
4 table holds encrypted communication path setting
5 information to be used for communication with a
6 communication partner in correspondence with the
7 communication partner IP address,

8 said communication encryption unit reads out
9 corresponding encrypted communication path setting
10 information from said encrypted communication path
11 setting table, encrypts the data packet in accordance
12 with the readout encrypted communication path setting
13 information, and transmits the data packet when the
14 communication partner IP address set as the destination
15 address of the received data packet is registered in
16 said encrypted communication path setting table,

17 said name resolution server comprises
18 a setting table which holds a correspondence
19 between a domain name condition to specify an encrypted
20 communication target node and encrypted communication

21 path setting information,
22 means, serving as said communication method
23 resolution unit, for determining whether the domain name
24 of said other node apparatus matches any one of domain
25 name conditions held in said setting table, and
26 a name resolution query/response
27 transmission/reception unit which adds encrypted
28 communication path setting information corresponding to
29 the matched domain name condition to the name resolution
30 response and transmits the name resolution response, and
31 said encrypted communication path setting unit
32 registers the encrypted communication path setting
33 information in said encrypted communication path setting
34 table in correspondence with the IP address of said
35 other node apparatus upon receiving the name resolution
36 response added the encrypted communication path setting
37 information from said name resolution server.

26. An encrypted communication system
2 according to claim 23, characterized in that said
3 communication method resolution unit determines whether
4 said other node apparatus is an encrypted communication
5 target node by looking up a setting table in which at
6 least part of the domain name of the encrypted
7 communication target node is registered.

27. An encrypted communication system
2 characterized by comprising:
3 a client node apparatus in which an

4 application that communicates with another node
5 apparatus connected to a network operates;
6 a communication encryption node apparatus
7 connected to said client node apparatus through the
8 network; and
9 a name resolution server which resolves an IP
10 address of each of said node apparatuses,
11 said communication encryption node apparatus
12 comprising
13 a data transmission/reception unit provided in
14 a kernel unit, and
15 a name resolution proxy unit which relays a
16 name resolution query transmitted from the application
17 to said name resolution server to resolve the IP address
18 of said other node apparatus and a name resolution
19 response as a response to the name resolution query,
20 said data transmission/reception unit
21 comprising
22 an encrypted communication path setting table
23 which holds a correspondence between a communication
24 partner IP address and an intercept address, and
25 a communication encryption unit which receives
26 a data packet transmitted from the application, reads
27 out, from said encrypted communication path setting
28 table, a communication partner IP address corresponding
29 to an intercept address set as a destination address of
30 the data packet, sets the readout communication partner

31 IP address as the destination address of the data
32 packet, and encrypts and transmits the set data packet,
33 said name resolution server comprising a
34 communication method resolution unit which determines on
35 the basis of a domain name of said other node apparatus
36 contained in one of the name resolution query and the
37 name resolution response whether said other node
38 apparatus is an encrypted communication target node, and
39 said name resolution proxy unit comprising
40 an encrypted communication path setting unit
41 which registers, in said encrypted communication path
42 setting table, a correspondence between the IP address
43 of said other node apparatus resolved by the name
44 resolution response and an intercept address that is not
45 used in any other communication session if said other
46 node apparatus is an encrypted communication target
47 node, and
48 a name resolution query/response
49 transmission/reception unit which transmits, to the
50 application as the name resolution response, the
51 intercept address corresponding to the IP address of
52 said other node apparatus contained in the name
53 resolution response received from the name resolution
54 server.

28. An encrypted communication system
2 according to claim 27, characterized in that said
3 encrypted communication path setting table holds a

4 plurality of correspondences between the communication
5 partner IP address and the intercept address.

29. An encrypted communication system
2 according to claim 27, characterized in that
3 said encrypted communication path setting
4 table holds encrypted communication path setting
5 information to be used for communication with a
6 communication partner in correspondence with the
7 communication partner IP address and the intercept
8 address,

9 said communication encryption unit reads out,
10 from said encrypted communication path setting table,
11 encrypted communication path setting information and the
12 communication partner IP address corresponding to the
13 intercept address set as the destination address of the
14 received data packet, encrypts the data packet having
15 the readout communication partner IP address set as the
16 destination address in accordance with the readout
17 encrypted communication path setting information, and
18 transmits the data packet,

19 said name resolution server comprises
20 a setting table which holds a correspondence
21 between a domain name condition to specify an encrypted
22 communication target node and encrypted communication
23 path setting information,

24 means, serving as said communication method
25 resolution unit, for determining whether the domain name

26 of said other node apparatus matches any one of domain
27 name conditions held in said setting table, and
28 a name resolution query/response
29 transmission/reception unit which adds encrypted
30 communication path setting information corresponding to
31 the matched domain name condition to the name resolution
32 response and transmits the name resolution response, and
33 said encrypted communication path setting unit
34 registers the encrypted communication path setting
35 information in said encrypted communication path setting
36 table in correspondence with the IP address of said
37 other node apparatus and the intercept address upon
38 receiving the name resolution response added the
39 encrypted communication path setting information from
40 said name resolution server.

30. An encrypted communication system
1 according to claim 27, characterized in that said
2 communication method resolution unit determines whether
3 said other node apparatus is an encrypted communication
4 target node by looking up a setting table in which at
5 least part of the domain name of the encrypted
6 communication target node is registered.

31. A program which causes a computer
2 included in a node apparatus in which an application
3 that communicates with another node apparatus connected
4 to a network operates to function as
5 communication encryption means provided in a

6 data transmission/reception unit of a kernel unit, and
7 name resolution proxy means for relaying a name
8 resolution query transmitted from the application to a
9 name resolution server to resolve an IP address of said
10 other node apparatus and a name resolution response as a
11 response to the name resolution query, characterized in
12 that

13 said communication encryption means receives a
14 data packet transmitted from the application and
15 encrypts and transmits the data packet when a
16 communication partner IP address set as the destination
17 address of the data packet is registered in an encrypted
18 communication path setting table that holds a
19 communication partner IP address, and

20 said name resolution proxy means comprises
21 encrypted communication path setting means for
22 registering, in the encrypted communication path setting
23 table, the IP address of said other node apparatus
24 resolved by the name resolution response if it is
25 determined on the basis of a domain name of said other
26 node apparatus contained in one of the name resolution
27 query and the name resolution response that said other
28 node apparatus is an encrypted communication target
29 node.

32. A program according to claim 31,
2 characterized in that the encrypted communication path
3 setting table holds a plurality of communication partner

4 IP addresses.

33. A program according to claim 31,
2 characterized in that said name resolution proxy means
3 further comprise communication method resolution means
4 for determining on the basis of the domain name of said
5 other node apparatus whether said other node apparatus
6 is an encrypted communication target node.

34. A program according to claim 33,
2 characterized in that
3 the encrypted communication path setting table
4 holds encrypted communication path setting information
5 to be used for communication with a communication
6 partner in correspondence with the communication partner
7 IP address,
8 said communication encryption means reads out
9 corresponding encrypted communication path setting
10 information from said encrypted communication path
11 setting table, encrypts the data packet in accordance
12 with the readout encrypted communication path setting
13 information, and transmits the data packet when the
14 communication partner IP address set as the destination
15 address of the received data packet is registered in
16 said encrypted communication path setting table,
17 said communication method resolution means
18 determines that said other node apparatus is an
19 encrypted communication target node when the domain name
20 of said other node apparatus matches any one of domain

21 name conditions held in a setting table that holds a
22 correspondence between a domain name condition to
23 specify an encrypted communication target node and
24 encrypted communication path setting information, and
25 said encrypted communication path setting
26 means registers, in the encrypted communication path
27 setting table, encrypted communication path setting
28 information corresponding to the matched domain name
29 condition in correspondence with the IP address of said
30 other node apparatus.

35. A program according to claim 31,
2 characterized in that said name resolution proxy means
3 further comprises name resolution query/response
4 transmission/reception means for transmitting, to the
5 name resolution server, the name resolution query
6 transmitted from the application to resolve the IP
7 address of said other node apparatus, receiving, from
8 the name resolution server, the name resolution response
9 containing a determination result indicating whether
10 said other node apparatus is an encrypted communication
11 target node and the IP address of said other node
12 apparatus, and transmitting, to the application, the
13 name resolution response containing the IP address of
14 said other node apparatus contained in the name
15 resolution response.

36. A program according to claim 35,
2 characterized in that

3 the encrypted communication path setting table
4 holds encrypted communication path setting information
5 to be used for communication with a communication
6 partner in correspondence with the communication partner
7 IP address,
8 said communication encryption means reads out
9 corresponding encrypted communication path setting
10 information from the encrypted communication path
11 setting table, encrypts the data packet in accordance
12 with the readout encrypted communication path setting
13 information, and transmits the data packet when the
14 communication partner IP address set as the destination
15 address of the received data packet is registered in the
16 encrypted communication path setting table,
17 said name resolution query/response
18 transmission/reception means receives, from the name
19 resolution server, the name resolution response further
20 containing encrypted communication path setting
21 information in addition to the determination result and
22 the IP address of said other node apparatus, and
23 said encrypted communication path setting
24 means registers, in the encrypted communication path
25 setting table, encrypted communication path setting
26 information contained in the name resolution response in
27 correspondence with the IP address of said other node
28 apparatus.

37. A program according to claim 33,

2 characterized in that said communication method
3 resolution means determines whether said other node
4 apparatus is an encrypted communication target node by
5 looking up a setting table in which at least part of the
6 domain name of the encrypted communication target node
7 is registered.

38. A program which causes a computer
2 included in a communication encryption node apparatus
3 connected, through a network, to a client node apparatus
4 in which an application that communicates with another
5 node apparatus connected to the network operates to
6 function as

7 communication encryption means provided in a
8 data transmission/reception unit of a kernel unit, and
9 name resolution proxy means for relaying a name
10 resolution query transmitted from the application to a
11 name resolution server to resolve an IP address of said
12 other node apparatus and a name resolution response as a
13 response to the name resolution query, characterized in
14 that

15 said communication encryption means receives a
16 data packet transmitted from the application, reads out,
17 from an encrypted communication path setting table that
18 holds a correspondence between a communication partner
19 IP address and an intercept address, a communication
20 partner IP address corresponding to an intercept address
21 set as a destination address of the data packet, sets

22 the readout communication partner IP address as the
23 destination address of the data packet, and encrypts and
24 transmits the set data packet, and
25 said name resolution proxy means comprises
26 encrypted communication path setting means for
27 registering, in the encrypted communication path setting
28 table, a correspondence between the IP address of said
29 other node apparatus resolved by the name resolution
30 response and an intercept address that is not used in
31 any other communication session if it is determined on
32 the basis of a domain name of said other node apparatus
33 contained in one of the name resolution query and the
34 name resolution response that said other node apparatus
35 is an encrypted communication target node, and
36 name resolution query/response
37 transmission/reception means for transmitting, to the
38 application as the name resolution response, the
39 intercept address corresponding to the IP address of
40 said other node apparatus contained in the name
41 resolution response received from the name resolution
42 server.

39. A program according to claim 38,
2 characterized in that the encrypted communication path
3 setting table holds a plurality of correspondences
4 between the communication partner IP address and the
5 intercept address.

40. A program according to claim 38,

2 characterized in that said name resolution proxy means
3 further comprises communication method resolution means
4 for determining on the basis of the domain name of said
5 other node apparatus whether said other node apparatus
6 is the encrypted communication target node.

41. A program according to claim 40,
2 characterized in that
3 the encrypted communication path setting table
4 holds encrypted communication path setting information
5 to be used for communication with a communication
6 partner in correspondence with the communication partner
7 IP address and the intercept address,
8 said communication encryption means reads out,
9 from the encrypted communication path setting table,
10 encrypted communication path setting information and the
11 communication partner IP address corresponding to the
12 intercept address set as the destination address of the
13 received data packet, encrypts the data packet having
14 the readout communication partner IP address set as the
15 destination address in accordance with the readout
16 encrypted communication path setting information, and
17 transmits the data packet,
18 said communication method resolution means
19 determines that said other node apparatus is an
20 encrypted communication target node when the domain name
21 of said other node apparatus matches any one of domain
22 name conditions held in a setting table that holds a

23 correspondence between a domain name condition to
24 specify an encrypted communication target node and
25 encrypted communication path setting information, and
26 said encrypted communication path setting
27 means registers, in the encrypted communication path
28 setting table, encrypted communication path setting
29 information corresponding to the matched domain name
30 condition in correspondence with the IP address of said
31 other node apparatus and the intercept address.

42. A program according to claim 38,
2 characterized in that said name resolution
3 query/response transmission/reception means transmits,
4 to the name resolution server, the name resolution query
5 transmitted from the application to resolve the IP
6 address of said other node apparatus, receives, from the
7 name resolution server, the name resolution response
8 containing a determination result indicating whether
9 said other node apparatus is an encrypted communication
10 target node and the IP address of said other node
11 apparatus, and replaces the IP address of said other
12 node apparatus contained in the name resolution response
13 with the intercept address and transmits the name
14 resolution response to the application if it is
15 determined that said other node apparatus is the
16 encrypted communication target node.

43. A program according to claim 42,
2 characterized in that

3 the encrypted communication path setting table
4 holds encrypted communication path setting information
5 to be used for communication with a communication
6 partner in correspondence with the communication partner
7 IP address and the intercept address,
8 said communication encryption means reads out,
9 from the encrypted communication path setting table,
10 encrypted communication path setting information and the
11 communication partner IP address corresponding to the
12 intercept address set as the destination address of the
13 received data packet, encrypts the data packet having
14 the readout communication partner IP address set as the
15 destination address in accordance with the readout
16 encrypted communication path setting information, and
17 transmits the data packet,
18 said name resolution query/response
19 transmission/reception means receives, from the name
20 resolution server, the name resolution response further
21 containing encrypted communication path setting
22 information in addition to the determination result and
23 the IP address of said other node apparatus, and
24 said encrypted communication path setting
25 means registers, in the encrypted communication path
26 setting table, encrypted communication path setting
27 information contained in the name resolution response in
28 correspondence with the IP address of said other node
29 apparatus and the intercept address.

44. A program according to claim 40,
2 characterized in that said communication method
3 resolution means determines whether said other node
4 apparatus is an encrypted communication target node by
5 looking up a setting table in which at least part of the
6 domain name of the encrypted communication target node
7 is registered.